

REMARKS

Claims 15-35 are pending in the present application, claims 34 and 35 having been added herein. The Office Action and cited references have been considered. Favorable reconsideration is respectfully requested.

Claim 16 was rejected due to a typographical error. This error has been corrected. Withdrawal of the rejection is respectfully requested.

Claim 32 has amended such that it is now distinguishable and not a duplicate of claim 23.

Claims 14-33 were rejected under U.S.C. § 101 because the claimed invention was allegedly directed to non-statutory subject matter. Claims 14-33 were also rejected under U.S.C. § 112, second paragraph. These rejections should be withdrawn for the following reasons. Claim 14 has been cancelled in favor of new claim 34, which is intended to overcome these rejections. In particular, claim 34 no longer refers generally to first and second electronic entities, but refers to a server entity and to a microcircuit entity, as discussed in particular from the bottom of page 1 and from line 18 of page 5 in the present application. Claim 34 also refers to a specific protocol, i.e., an authentication protocol, as discussed on page 1, at the bottom of the page, which results in the validation of the authentication when the results are identical (see page 2, lines 10-11). Further, claim 34 states that first chain of operations is part of a DES and is stored in both entities (see page 5, lines 22-23 and lines 28-30). Further, claim 34 recites that the attack is of the DPA type, as explained at the bottom of page 2 and states which entity operates a given step, as explained in the detailed description of the application.

Additional claim 35 has been added which differs from claim 34 in that it recites, as explained in connection with figure 1 of the present application, that there is, in the microcircuit entity, the same first chain as in the server entity, as well as a complemented chain of operations, and the microcircuit entity applies to the message a modified chain of operations consisting of operations selected from either the first chain of operations or from the complemented chain of operations. Applicant respectfully submits that the present wording of independent claims 25, 34 and 35 refer to a tangible method, operated within server or microcircuit entities, with the result that an authentication is validated depending on whether or not the result from both entities are identical.

Based on these amendments, Applicant respectfully submits that claim 14 satisfies 35 U.S.C. § 101 as providing a useful, concrete and tangible result. Additionally, claim 14 has believed to be to satisfy 35 U.S.C. § 112, second paragraph. Other amendments have been made to the dependent claims to overcome the rejections set forth on pages 8-10 of the previous Office Action. Withdrawal of these rejections are respectfully requested.

Claims 14-33 were rejected under rejected under U.S.C. § 103 as being unpatentable over Applicant's admitted prior art (AAPA) in view of Kocher (U.S. Patent No. 6,278,783) and Chow (U.S. Patent No. 6,594,761). This rejection is respectfully traversed.

Claim 34 recites a method of performing an authentication cryptographic protocol between a server entity and a microcircuit entity in order to resist a DPA attack against the microcircuit entity during performing this authentication cryptographic protocol, comprising the steps of storing a DES comprising a first chain of operations in both the server entity and the microcircuit entity, having a message exchanged between this server entity and this microcircuit entity, and having the server entity apply to the message the first chain of operations which is stored therein so as to obtain a server result, and having the microcircuit

entity determine a second chain of operations from the first chain of operations which is stored in this microcircuit entity. This second chain of operations comprises a succession of operations each corresponding to a corresponding operation in the first chain of operations with each operation of the second chain of operations being the corresponding operation of the first chain of operations either in the same state or in the complemented state. The step of having the microcircuit entity determine the second chain of operations from the first chain of operations comprises a step of randomly selecting, for at least a part of the second chain of operations corresponding to a corresponding part of the first chain of operations, either this at least a part of the operations of the first chain of operations in a same state as in the first chain of operations, or this at least a part of the first chain of operations in a complemented state. The step of having the microcircuit entity determine the second chain of operations is such that at least some of the operations of this second chain of operations are in the same state as the corresponding operations in the first chain of operations whereas the other operations of this second chain of operations are in complemented state with respect to the corresponding operations of the first chain of operations. The method further comprises having the microcircuit card apply this second chain of operations to the message so as to obtain a resultant message. The step of having the microcircuit apply this second chain of operations comprises a step of selecting to output as the resultant message, depending on the step of having the microcircuit entity determine the second chain of operations, one of either the result of a last operation of the second chain of operations in a same state or the result of this last operation of the second chain of operation in a complemented state, and comparing the resultant message obtained from the second chain of operations to the server result. The method further comprises validating the authentication between the server entity and the

microcircuit entity when the server result and the resultant message are identical. This is not taught, disclosed or made obvious by the prior art of record.

As far as the prior art is concerned, Applicant respectfully submits that the features of claims 25, 34 and 35 are not taught or suggested by Kocher and/or Chow. Applicant has presented arguments in the previous response, which are incorporated by reference herein, explaining that both Chow and Kocher include teachings which do not lead the person skilled person in the art to the invention. As a matter of fact, these documents relate to several ways to proceed which are sufficiently different such a person skilled in the art would have been unable to determine which features to take from each document for improving the admitted prior art. Applicant respectfully submits that the selection of features made by the Examiner is made with an improper hindsight view of the invention to find elements in the prior art which anticipate the claimed features, whereas the inventive activity of the invention must be analyzed in view of only the information and hints available before the invention.

In particular, it is to be noted that, if Kocher teaches that some step is conducted randomly, it fails to teach or suggest to include randomness in the particular step of selecting to take an operation in a normal state or in a complemented state.

In fact, Applicant submits that this feature is not taught in the prior art whether taken alone or in combination as suggested in the Office Action. The Office Action on page 3-4 inserts that

Kocher is relied on upon for a teaching of determining what operations to perform based on a random determination (column 9, lines 1-13 as cited), and in combination with the disclosure of Chow, this suggests determining whether the complement of an operation is to be performed based on a random determination.

Applicant respectfully disagrees. In particular, Kocher at the cited portion, states

to transform the message M, the device obtains a random 64-bit value or, computes $M1=M \text{ XOR } R$ and $M2=R$, creates randomized permutations $M1P$ and $M2P$, permutes $M1$ and $M2$ according to the inverses of $M1P$ and $M2P$...

This is not a teaching of determining what operation to perform based on a random determination. Although the value R is a random number, the operation performed is always the same. Thus, Kocher does not suggest the step of randomly selecting, for at least a part of the second chain of operations..., either this at least a part of the operations of the first chain of operations in a same state as in the first chain of operations, or this at least a part of the first chain of operations in complemented state, as recited in claim 34. For at least these reasons, Applicant respectfully submits that claim 34 is patentable over the prior art of record.

Claims 25 and 35 are believed to patentable at least for the reasons discussed above with respect to claim 34. Claims 15-24 and 26-33 depend from and includes the recitations of claims 34. Applicant respectfully submits that these claims are patentable in and of themselves and for the reasons discussed above with respect to claim 34.

In view of the above amendments and remarks, Applicant respectfully requests reconsideration and withdrawal of the outstanding rejections of record. Applicant submits that the application is in condition for allowance and early notice to this effect is most earnestly solicited.

If the Examiner has any questions he is invited to contact the undersigned at 202-628-5197.

Appln. No. 09/771,967
Amd. dated October 1, 2007
Reply to Office Action of March 30, 2007

Respectfully submitted,

BROWDY AND NEIMARK, P.L.L.C.
Attorneys for Applicant

By /Ronni S. Jillions/
Ronni S. Jillions
Registration No. 31,979

RSJ:srd
Telephone No.: (202) 628-5197
Facsimile No.: (202) 737-3528
G:\BN\B\Bonn\Akkar1\pto\2007-10-01AMD.doc